Application No.:09/940,706
Filing Date: 08/28/2001

Docket No.: JP920010196US1

IN THE CLAIMS

Please amend the claims as set out below:

1. (currently amended) ~~In a~~ A method for providing secure authentication, ~~using digital certificates, an improvement to enable the selective transfer of authentication data~~ the method comprising:

a) ~~presentation of~~receiving basic authentication data from a first computer for a secure transaction between the first computer and a second computer, wherein the receiving is by the second computer, the secure transaction is during a certain communication session between the first and second computer, and the basic authentication data has been certified by an accepted certifying authority, and wherein the basic authentication data includes a public key of the first computer for permitting a first type of access by the first computer to an application provided by the second computer;~~, at the commencement of a secure transaction,~~

b) storing a copy of the first computer's public key;

c) requesting, by the second computer during the communication session, an additional individual authentication data unit from the first computer, wherein the additional individual authentication data unit is for permitting a second type of access by the first computer to an application provided by the second computer;

d) ~~transfer of~~receiving the additional individual authentication data unit~~s~~ by the second computer from the first computer~~against specific requests~~; and

e) verifying authenticity of the additional individual authentication data unit, wherein c) includes storing the first computer's public key by the second computer during the certain communication session, and the verifying includes verifying the additional individual authentication data unit by the second computer using the second computer's stored copy of the first computer's public key during the certain communication session and without the second computer obtaining another copy of the public key. ~~as and when required,~~

~~thereby eliminating the risks associated with providing any authentication data that is not required for a particular transaction.~~

2. (currently amended) The improved method as claimed in claim 1 wherein the second type of access includes an access for an application in which a digital credit card is used for a purchase.~~authenticity of said additional individual authentication data is established by using the public key provided in said basic authentication data.~~

3. (currently amended) The ~~improved~~ method as claimed in claim 1, wherein the authenticity of said additional individual authentication data is established by signature of said accepted certifying authority.

4. (currently amended) The improved method as claimed in claim 1 wherein the second type of access includes an access for an application in which an email message is securely transmitted. ~~said additional individual authentication data is provided without the need for establishing a separate session.~~

5. (currently amended) The improved method as claimed in claim 1, wherein the authentication data includes an identity certificate, and the method includes:

receiving, by the second computer, a command from the first computer for the second computer to invalidate a previously presented identity certificate; and

receiving, by the second computer, a new identity certificate from the first computer to replace the invalidated identity certificate, wherein the command to invalidate and the new identity certificate are both received by the second computer during the certain communication session.~~further comprising the facility to invalidate previously presented authentication data and present new authentication data and present new authentication data as and when required, thereby enabling establishment of new transactions without the need for closing an existing session.~~

6. (currently amended) ~~In a~~A system for providing secure authentication, ~~using digital certificates, an improvement to enable the selective transfer of authentication data~~ the system comprising:

means for ~~presenting~~receiving basic authentication data from a first computer for a secure transaction between the first computer and a second computer, wherein the receiving is by the second computer, the secure transaction is during a certain communication session between the first and second computer, and the basic authentication data has been certified by an accepted certifying authority, and wherein the basic authentication data includes a public key of the first computer for permitting a first type of access by the first computer to an application provided by the second computer ~~at the commencement of a secure transaction;~~

means for storing a copy of the first computer's public key;

means for requesting, by the second computer during the communication session, an additional individual authentication data unit from the first computer, wherein the additional individual authentication data unit is for permitting a second type of access by the first computer to an application provided by the second computer;

means for receiving the ~~transferring~~ additional individual authentication data units by the second computer from the first computer; and ~~against specific requests, as and when required,~~

means for verifying authenticity of the additional individual authentication data unit, wherein the storing means includes means for storing the first computer's public key by the second computer during the certain communication session, and the means for verifying includes means for verifying the additional individual authentication data unit by the second computer using the second computer's stored copy of the first computer's public key during the certain communication session and without the second computer obtaining another copy of the public key.

~~thereby eliminating the risks associated with providing any authentication data that is not required for a particular transaction.~~

7. (currently amended) The ~~improved~~ system as claimed in claim 6 wherein the second type of access includes an access for an application in which a digital credit card is used for a purchase ~~authenticity of said additional individual authentication data is established by using the public key provided in said basic authentication data.~~

8. (currently amended) The ~~improved~~ system as claimed in claim 6, wherein the authenticity of said additional individual authentication data is established by means of signature of said accepted certifying authority.

9. (currently amended) The ~~improved~~ system as claimed in claim 6, wherein the second type of access includes an access for an application in which an email message is securely transmitted. ~~said additional individual authentication data is provided without the need for establishing a separate session.~~

10. (currently amended) The ~~improved~~ system as claimed in claim 6, wherein the authentication data includes an identity certificate, and the system includes:

means for receiving, by the second computer, a command from the first computer for the second computer to invalidate a previously presented identity certificate; and

means for receiving, by the second computer, a new identity certificate from the first computer to replace the invalidated identity certificate, wherein the command to invalidate and the new identity certificate are both received by the second computer during the certain communication session.~~further comprising the means for invalidating previously presented authentication data and present new authentication data and present new authentication data as and when required, thereby enabling establishment of new transactions without the need for closing an existing session.~~

11. (currently amended) A~~In a~~ computer program product comprising computer readable program code stored on computer readable storage medium embodied therein for providing secure authentication, ~~using digital certificates, an improvement to enable the selective transfer of authentication data~~the computer program product comprising:

computer readable program code means configured for ~~presenting~~ receiving basic authentication data from a first computer for a secure transaction between the first computer and a second computer, wherein the receiving is by the second computer, the secure transaction is during a certain communication session between the first and second computer, and the basic authentication data has been certified by an accepted certifying authority, and wherein the basic

authentication data includes a public key of the first computer for permitting a first type of access by the first computer to an application provided by the second computer;~~at the commencement of a secure transaction;~~

computer readable program code means configured for storing a copy of the first computer's public key;

computer readable program code means configured for requesting, by the second computer during the communication session, an additional individual authentication data unit from the first computer, wherein the additional individual authentication data unit is for permitting a second type of access by the first computer to an application provided by the second computer;

computer readable program code means configured for ~~transferring~~receiving the additional individual authentication data units by the second computer from the first computer; and ~~against specific requests, as and when required;~~

computer readable program code means configured for verifying authenticity of the additional individual authentication data unit, wherein the computer readable program code means configured for storing a copy of the first computer's public key includes computer readable program code means configured for storing the first computer's public key by the second computer during the certain communication session, and the verifying includes verifying the additional individual authentication data unit by the second computer using the second computer's stored copy of the first computer's public key during the certain communication session and without the second computer obtaining another copy of the public key.~~thereby eliminating the risks associated with providing any authentication data that is not required for a particular transaction.~~

12. (currently amended) The ~~improved~~ computer program product as claimed in claim 11, wherein the second type of access includes an access for an application in which a digital credit card is used for a purchase.~~authenticity of said additional individual authentication data is established by using the public key provided in said basic authentication data.~~

13. (currently amended) The ~~improved~~ computer program product as claimed in claim 11, wherein the authenticity of said additional individual authentication data is established by signature of said accepted certifying authority.

14. (currently amended) The ~~improved~~ computer program product as claimed in claim 11, wherein the second type of access includes an access for an application in which a digital credit card is used for a purchase, ~~said additional individual authentication data is provided without the need for establishing a separate session.~~

15. (currently amended) The ~~improved~~ computer program product as claimed in claim 11, wherein the authentication data includes an identity certificate, and the computer program product includes:

computer readable program code means configured for receiving, by the second computer, a command from the first computer for the second computer to invalidate a previously presented identity certificate; and

computer readable program code means configured for receiving, by the second computer, a new identity certificate from the first computer to replace the invalidated identity certificate, wherein the command to invalidate and the new identity certificate are both received by the second computer during the certain communication session. ~~further comprising the computer readable program code means configured for invalidating previously presented authentication data and present new authentication data and present new authentication data as and when required, thereby enabling establishment of new transactions without the need for closing an existing session.~~